



USAID
FROM THE AMERICAN PEOPLE

THE USAID SECURING GEORGIA'S
ENERGY FUTURE PROGRAM



GOVERNANCE FRAMEWORK TO PROMOTE A CYBER-SECURE ENERGY SECTOR

THE USAID SECURING GEORGIA'S ENERGY FUTURE PROGRAM

MARCH 2, 2022

DISCLAIMER: This report was produced for review by the United States Agency for International Development. It was prepared by Deloitte Consulting LLP. The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

GOVERNANCE FRAMEWORK TO PROMOTE A CYBER-SECURE ENERGY SECTOR

THE USAID SECURING GEORGIA'S ENERGY FUTURE
PROGRAM

MARCH 2, 2022

THE USAID SECURING GEORGIA'S ENERGY FUTURE PROGRAM

CONTRACT NUMBER: 7200AAI9D00025

TASK ORDER NUMBER: 7201I42IF00002

DELOITTE CONSULTING LLP

USAID | GEORGIA

DISCLAIMER: This report was produced for review by the United States Agency for International Development. It was prepared by Deloitte Consulting LLP. The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

ACRONYMS

CCGT	Combined Cycle Power Plant
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CISA	Certified Information System Auditor
CSB	Cyber Security Bureau
CSIRT	Computer Security and Incident Response Team
DGA	Digital Governance Agency
EPG	Energopro Georgia
ESCO	Electricity Market Operator
EU	European Union
GCGC	Georgian Cross Government Cyber working group
GENEX	Georgian Energy Exchange
GGTC	Georgian Gas Transportation Company
GNCC	Georgian National Communication Commission
GNERC	Georgian National Energy and Water Supply Regulatory Commission
GoG	Government of Georgia
GOGC	Georgian Oil and Gas Corporation
GSE	Georgian State Electrosystem
HPP	Hydro Power Plant
ICT	Information Communication Technologies
ISACA	Information Systems Audit and Control Association
ISL	Information Security Law of Georgia
ISO	International Organization for Standardization
IT	Information Technology
kV	Kilovolt
LEPL	Legal Entity of Public Law
MISP	Malware Information Sharing Platform
MoD	Ministry of Defense of Georgia
MoJ	Ministry of Justice of Georgia
MW	Megawatt
NBG	National Bank of Georgia
NIST	National Institute of Standards and Technology
NSC	National Security Council
NSMP	North-South Main Gas Pipeline
OTA	Operational-Technical Agency
SCADA	Supervisory Control and Data Acquisition
SCP	South Caucasus Pipeline
SOCAR	State Oil Company of Azerbaijan Republic
SSSG	State Security Service of Georgia
TPP	Thermal Power Plant
TYNDP	Ten Year Network Development Plan
USAID	United States Agency for International Development

TABLE OF CONTENTS

I	INTRODUCTION.....	3
2	EXECUTIVE SUMMARY	4
3	GEORGIA’S CYBERSECURITY GOVERNANCE FRAMEWORK.....	6
	3.1 National Cybersecurity Authorities	7
	3.2 Sector Specific Regulatory Authorities	9
	3.3 Additional Cyber Stakeholders	9
	3.4 Consultative Bodies, Public-Private Cooperation Forums	9
	3.5 Critical Information Infrastructure	10
4	RECOMMENDATIONS	12
5	ANNEXES.....	14
	Annex I: Definition of Critical Information Infrastructure	14
	Annex II: Methodology for Critical Information Infrastructure Identification	15
	Annex III: CII in the Georgian Energy Sector	16
	Annex IV: Key CII Obligations, Supervisory Authority Responsibilities	18
	Annex V: References	19

I INTRODUCTION

The following report is offered pursuant to Contract 7200AA19D00025/72011421F00002 between USAID/Georgia and Deloitte Consulting LLP (the “Contract”) for the USAID Securing Georgia’s Energy Future Program (the “Program”).

The Program’s aim is to support the development of Georgia’s energy sector into an open, regionally integrated, market-driven system capable of independently planning, financing, and implementing solutions to Georgia’s energy security challenges, and thereby improving the enabling environment for private energy investments. The specific Program Objectives are:

- i. **Improved Energy System Planning:** Build the capacity of the Government of Georgia (GoG) and associated energy sector institutions to establish, coordinate, and enforce energy sector policy, primarily through approaches that will improve sector planning capabilities.
- ii. **Increased Investment to Promote Energy Sector Resilience:** In coordination with steps to align Georgia’s energy market rules with European Union (EU) Directives and build the capacity of Georgian energy sector entities to operate in advanced market structures, this activity supports private engagement to assist Georgia in attracting energy sector investment.
- iii. **Improved Governance and Operations of Well-Functioning Georgian Energy Market:** Build the capacity of Georgian institutions responsible for energy market governance to successfully facilitate Georgia’s transition to a fully functioning, liquid energy market; and broaden Georgia’s regional energy market integration and cross-border trade with Azerbaijan, Armenia, and Turkey (and ultimately expand physical and commercial linkages to and with EU markets).
- iv. **Reduced Cybersecurity Vulnerabilities:** Build upon prior USAID assistance to bolster the capacity of energy sector stakeholders and institutions, principally energy utilities, to increase the resilience of the critical infrastructure of Georgia’s energy sector and, in so doing, safeguard the strategic segments of the national economy and the country as a whole.

Per deliverable 4.2.4.2 of the Contract, the Program has compiled a report titled *Governance Framework to Promote a Cyber-secure Energy Sector*. The report contains a description of the existing cyber governance framework in the Georgian energy sector, identifies gaps in its current structure and provides recommendations to improve existing cyber practices.

A report titled *Identification of Critical Energy Sector Cybersecurity Infrastructures* in Annex II of this report further elaborates on these recommendations, proposing a methodology to amend the existing list of Critical Information Infrastructures (CII) recently approved by the GoG and to add a series of energy entities the Program believes should be included on the list.

This report contains five sections including the **Introduction (1)** and **Executive Summary (2)**.

Georgia’s Cybersecurity Governance Framework (3) contains a comprehensive overview of the existing cybersecurity governance framework. **Areas for Further Improvement (4)** presents the Program’s recommendations on how to address gaps in the current cybersecurity governance framework. **Annexes (5)** contains additional analytical: Definition of Critical Information Infrastructure (Annex I); Methodology for Identifying Critical Information Infrastructure (Annex II); Georgian Energy Sector’s Critical Information Infrastructures (Annex III), References (Annex IV) and a longer discussion of CII obligations and their supervisory authorities’ duties (Annex V).

2 EXECUTIVE SUMMARY

Cybersecurity is one of Georgia's top national security concerns. This is especially the case in the energy sector as it provides essential services for other sectors of the economy. Cyber disruption of the energy sector could trigger cascade effects in other sectors of the economy and cause devastating fallout for the country at large. To assist in the navigation of current threats in cyber space this report reviews current Georgia's cybersecurity governance framework, provides guidance to energy sector stakeholders in negotiating the framework and suggests a methodology to identify entities that should be deemed CII and obliged to abide by stricter standards of cybersecurity.

Georgia currently takes a multiple competent authority approach to cybersecurity with several regulatory actors responsible for CII entities in various sectors. While a list of CII entities existed in earlier years, it contained only state entities, and there was just one all-encompassing category of CII. Starting in 2022, the scope of CII was expanded to include three separate categories. As a result, a number of other public and private energy sector assets were included on the list of CII.

There are four main national bodies which are responsible for various aspects of cybersecurity in Georgia:

- **The National Security Council (NSC)** is the key state authority responsible for political and strategic level cybersecurity governance; the council is authorized to coordinate a national response to cyber-incidents which threaten state or public interests
- **The Digital Governance Agency (DGA)** is responsible for cyber issues amongst private sector CII entities
- **The Operative-Technical Agency (OTA)** is responsible for carrying out covert investigative activities and electronic surveillance measures. The OTA's scope of operation covers public sector CII as well as internet service providers
- **The Cyber Security Bureau (CSB)** is a legal entity of public law (LEPL) under the Ministry of Defense of Georgia (MoD) whose mandate is to develop robust information and cybersecurity systems and to minimize the consequences of cyberattacks which target defense sector CII.

In addition, there are three sector-specific cyber competent authorities:

- the National Bank of Georgia (NBG)
- the Georgian National Energy and Water Supply Regulatory Commission (GNERC), and
- the Georgian National Communication Commission (GNCC).

The Georgian cybersecurity governance framework is built around the concept of CII entities signed into law by the Prime Minister's Order of December 31, 2021. The act defines CII as 'public and private entities whose uninterrupted operations of their information systems are essential to the defense and/or economic security of the state, and the maintenance of state authority and/or public life.' There are three categories of CII:

- **Category 1** CII are public bodies, mainly ministries, LEPLs, the presidential and government administrations, the Parliament of Georgia, the State Elections Committee, State Security Service of Georgia (SSSG), Tbilisi City Hall, and several state-owned companies (e.g. Georgian Post, Georgian Railway, Sakaeronavigatsia). These CII fall under the supervision of the OTA
- **Category 2** CII include major internet service provider companies, e.g., Magticom, Silknet, and Caucasus Online. This category is also under OTA's supervision
- **Category 3** CII includes commercial banks, insurance companies, seaports, sea, air and land transportation, and energy sector entities. DGA oversees Category 3 CII.

There are some shortcomings in Georgia's current cybersecurity governance framework. To address these gaps, the Program recommends to:

- clarify and operationalize the current cybersecurity governance framework
- formulate rules and methodology for identifying CII
- address diverging standards and uneven compliance costs across CII categories within the same sector, and
- expand the list of CII to include missing energy entities as recommended in this report.

Implementation of these recommendations will provide a more consistent approach to energy cybersecurity governance and enable the development of a more resilient cybersecurity framework for Georgia.

3 GEORGIA'S CYBERSECURITY GOVERNANCE FRAMEWORK

The number of active cyber threats means cybersecurity is at the top of Georgia's list of national security concerns. The energy sector is especially vulnerable given its complexity and how critical energy supply is to other sectors. Potential cyber disruption of the energy sector could trigger a cascade effect in other sectors of the economy causing devastating fallout for the country at large. Therefore, it is important to understand shortcomings in Georgia's current approach to cybersecurity governance, which this analysis aims to achieve by reviewing the country's cyber framework.

Cybersecurity governance frameworks can be wide-reaching in scope, but broadly attempt to create institutions with mandates to:

- establish information and cybersecurity measures
- provide access to technical support, advisory and awareness-raising services
- address cyber incidents and threats
- conduct information and cyber audits, and
- help identify CII entities and enforce supervisory mechanisms.

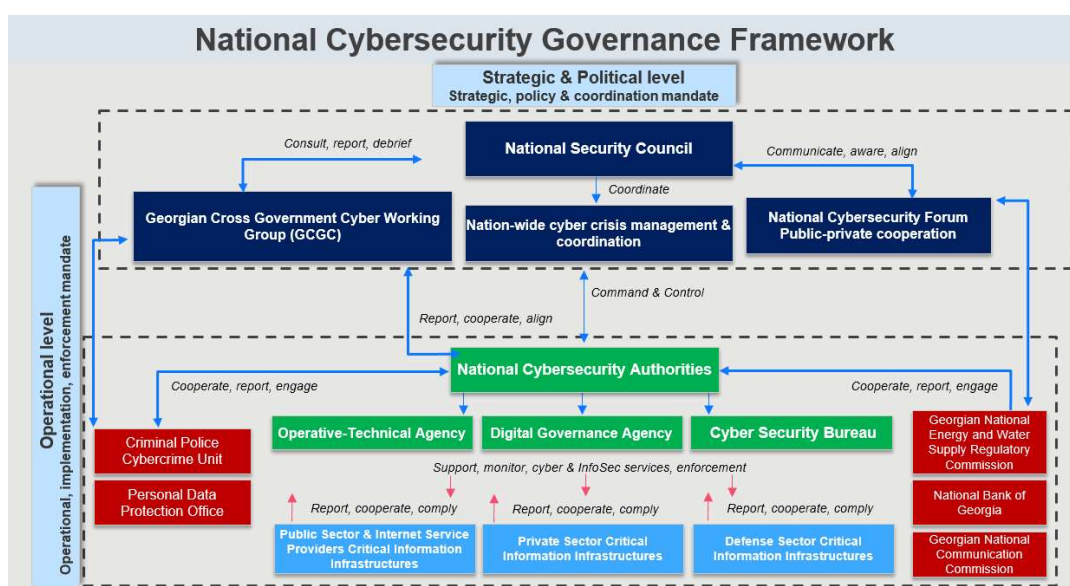
Cybersecurity governance frameworks can be divided into approaches with:

- a highly centralized, single competent authority, or
- multiple competent authorities

Industry consensus is that there is no one-size-fits-all approach. In either case, a clear governance system and distinctive supervisory mandates are key to developing a sustainable cybersecurity environment.

Georgia's cybersecurity governance framework has dramatically transformed over the previous decade. Cybersecurity in Georgia has historically been the domain of national security authorities and less that of individual businesses. The frequent restructuring of organizations overseeing cybersecurity and the absence of coordination amongst them has been an impediment to the development of cybersecurity. State institutions are still working to further shape and regulate the country's cybersecurity governance framework with the aim of codifying the standards by which CII entities must abide. These regulations are imposed in a top-down manner. Figure I below illustrates the current configuration of Georgia's cybersecurity governance framework and hierarchical relations between CII entities and their supervisory authorities.

Figure I: Georgian Cybersecurity Governance Framework



3.1 NATIONAL CYBERSECURITY AUTHORITIES

There are four main bodies which oversee the implementation of national cybersecurity policy in Georgia. Their mandate and activities are outlined below.

i. National Security Council

The National Security Council (NSC) is broadly responsible for Georgia's security concerns. Its cybersecurity unit is the Information and Cybersecurity Department and is the key state authority responsible for political and strategic level cybersecurity governance. It was re-established¹ in 2019 by the Law of Georgia on Planning and Coordination Rules of National Security Policy under the Georgian Prime Minister's Office.

The council both serves as an analytical think tank and strategic coordination body and is the nation-wide cyber incident management authority. The NSC plans and coordinates information and cybersecurity policy, conducts analytical cyber research and situational analyses of cyber threats, and carries out cyber risk mitigation activities. Moreover, the NSC oversees the coordination and implementation of the Action Plan of the National Cybersecurity Strategy.

Coordination of a national response to cyber-incidents which threaten state or public interests and management of any crisis caused by such cyber incidents on the decision-making level are the domain of the NSC. Furthermore, the NSC develops response plans and recommendations against cyber threats and attacks, guides the national competent cyber authorities and orchestrates their work.

Awareness raising is an important defensive mechanism at the disposal of the NSC. The NSC is charged to raise awareness about proactive steps which can counter risks and threats in the cyber landscape. Supporting information sharing and facilitating coordination between competent authorities – CERT (Computer Emergency Response Team) / Computer Security and Incident Response Teams (CSIRTs), law enforcement and cyber-defense, regulatory bodies and CII – is another crucial day-to-day duty of the NSC.

While the NSC sets strategic and political priorities in the field of cybersecurity, enforcement falls under the mandate of the national cybersecurity competent authorities outlined below.

ii. Digital Governance Agency

The Digital Governance Agency (DGA) is the legal successor of the Data Exchange Agency, the first cybersecurity authority in Georgia. Structural and institutional reforms transformed the Data Exchange Agency into the Digital Governance Agency in June 2020. The DGA is subordinate to the Ministry of Justice of Georgia (MoJ).

The DGA is responsible for cyber issues in private sector critical information infrastructure. The agency's key mandate is to develop a common legal and regulatory framework for the protection of private sector critical infrastructure, including entities in the energy sector. The DGA also oversees the introduction of digital services and systems.

The DGA:

- defines rules for audit and penetration testing
- sets minimum requirements for information security policies
- reviews internal security policies of CIIs

¹ The Georgian NSC has existed in several manifestations over the last two decades, under either the president's or the PM's jurisdiction. The most recent iteration dates to 2019.

- conducts cybersecurity services and compliance checks
- manages incident reporting mechanisms and handles cyber incidents
- monitors and enforces compliance of CII with the requirements of the Information Security Law (ISL) of Georgia

The DGA's information and cybersecurity competencies mainly pertain to day-to-day cybersecurity capacity building to strengthen private sector CII systems, support the development of their cybersecurity capacity and enhance their resilience against cybersecurity threats and attacks. The agency's back-office operations unit CERT.DGA.GOV.GE is largely responsible for these activities. The main function of CERT.DGA.GOV.GE is to offer consulting and advisory services regarding cyber incidents, monitor the cyber environment in the private critical sectors, register and analyze existing and potential cyber threats, and provide recommendations on how to avoid and neutralize them.

Cyber and information security awareness are another important aspect of the DGA's activities. The agency is also an active member of all major international organizations in the information and cybersecurity industry.

iii. Operative-Technical Agency

The Operative-Technical Agency (OTA) is a LEPL created in 2017 under the State Security Service of Georgia.

The agency's responsibilities include carrying out covert investigative activities and electronic surveillance measures when requested to do so by investigative, intelligence and counterintelligence agencies. The OTA's cybersecurity mandate is outlined by ISL amendments from June 2021, and its scope of operation covers public sector CII as well as internet service providers.

OTA's operations unit CERT.OTA.GOV.GE is mandated to act as the authority for managing cybersecurity incidents within state CII networks and at the level of internet service providers. Incident handling, response and recovery are the key daily activities of CERT. OTA's information and cybersecurity mandates are relatively new in comparison with other operations level stakeholders; the agency is currently expanding its human resources and technical capacity to meet its cybersecurity mandate.

iv. Cyber Security Bureau

The Cyber Security Bureau (CSB) is an LEPL under the Ministry of Defense created in 2014. The mission of the bureau is to develop robust information and cybersecurity systems and to minimize harmful consequences of cyberattacks which target defense sector CII.

The CSB implements preventative and responsive measures to manage targeted threats against information security, and to respond to cyberattacks and security incidents. The CSB also defines and develops defense information security policies and sets minimum information security requirements. It is authorized to develop concept and regulatory documents, legal frameworks, and ensure compatibility with international standards and legal norms in the cybersecurity field.

The bureau works closely with NATO and its partners, participates in various NATO-led cyber exercises and capacity building initiatives. It also has access to NATO's Malware Information Sharing Platform (MISP). CSB drafts list of CII in the defense sector. The CSB is vested with a full information and cybersecurity mandate both on the operations and supervisory level in the defense sector.

3.2 SECTOR SPECIFIC REGULATORY AUTHORITIES

There are three sector-specific cyber competent authorities:

- **NBG** has cyber authority in the banking sector, setting minimum requirements for information security policies, responding to cases of non-compliance, and providing audit process and asset management
- **GNERC** is a cyber stakeholder in the energy and water sectors
- **GNCC** is a cyber stakeholder in the telecommunications field.

Although GNERC and GNCC's mandates are not yet defined, their role includes information sharing, notification of incidents, sector-specific reporting and acting as communication mediators between CILs and national cyber authorities.²

3.3 ADDITIONAL CYBER STAKEHOLDERS

There are several additional cyber stakeholders with important roles in the implementation of cyber security:

- The Ministry of Internal Affairs is responsible for cybercrime law enforcement, carried out through the Cybercrime Division within the Central Criminal Police Department created in 2012. The department also serves as Georgia's 24/7 international contact point for cybercrime investigation and cooperation.
- The Personal Data Protection Office, an independent state authority, plays a crucial role in protecting the data of individuals in the cyber domain and is an important stakeholder within the cybersecurity governance system. According to the new Law on Personal Data Protection, the Personal Data Protection office is responsible for:
 - supervising the implementation of data protection legislation
 - monitoring and enforcing the law
 - providing instructions to the public and the private sector about how to ensure adequate protection of personal data
 - reviewing data-related complaints and appeals
 - inspecting public and private entities to ensure that the data processing is carried out in compliance with the law, and
 - raising public awareness on the protection of personal data, and
 - protecting personal data rights in cyber space.

3.4 CONSULTATIVE BODIES, PUBLIC-PRIVATE COOPERATION FORUMS

In addition to national cyber competent authorities and sectoral regulatory bodies, Georgia's cybersecurity governance framework includes public-private cooperation platforms and other consultative bodies.

The National Cybersecurity Forum is an annual event which serves as a platform for sharing ideas on challenges and opportunities for Georgia within the cyber domain. The primary goal of the

² Some countries have energy sector authorities that are designated CSIRT/CERTs for the energy sector, e.g., Austria, Norway and UK. Austria's energy CERT has an important role in increasing resilience against cyberattacks in the Austrian energy industry. In addition, some energy CILs in Italy have a CERT. In particular, Italian energy company Enel has a division - CERTI9, which has the mission to support and protect the company from intentional and malicious attacks that would hamper its constituency.

Cybersecurity Forum is to enable public-private discussions about the national cybersecurity environment and propose solutions to problematic issues.

The Georgian Cross Government Cyber (GCGC) working group is an inter-agency forum where all cyber authorities can discuss national cybersecurity topics, the implementation of the National Cybersecurity Strategy and its Action Plan, and other various aspects of ongoing reforms in the field of cybersecurity. The meetings of the GCGC are regular. Both the GCGC and Cyber Security Forum are organized and hosted by the NCS.

3.5 CRITICAL INFORMATION INFRASTRUCTURE

The Georgian cybersecurity governance framework is built around the concept of entities of Critical Information Infrastructure signed into law by the Prime Minister's Order of December 31, 2021.

The act defines CII as 'public and private entities whose uninterrupted operations of their information systems are essential to the defense and/or economic security of the state, and the maintenance of state authority and/or public life.' The ISL reads that the Ministry of Justice drafts the list of CII in agreement with the MoD and MIA, NSC and the SSS, who then submits the list to the GoG for approval.

General criteria defining what constitutes a CII are also issued by the ISL of Georgia. They include:

- the scale of potential consequences resulting from the malfunction or the failure of an information system
- the scale of expected economic losses for CII and/or the State
- the necessity of services delivered by the information system for the normal functioning of society
- the number of information system users
- economic conditions of the CII, and
- the amount of estimated costs incurred as a result of the information and cybersecurity obligations imposed by ISL

There are three categories of CII:

- I. **Category 1 CII** are public bodies, mainly ministries, LEPLs, the presidential and government administrations, the Parliament of Georgia, the State Elections Committee, SSSG, Tbilisi City Hall, and several state-owned companies (e.g., Georgian Post, Georgian Railway, Sakaeronavigatsia). These CII fall under the supervision of the OTA.
- II. **Category 2 CII** includes major internet service provider companies, e.g., Magticom, Silknet, and Caucasus Online. This category is also under OTA's supervision.
- III. **Category 3 CII** includes commercial banks, insurance companies, seaports, sea, air and land transportation, and energy sector entities. These are overseen by the DGA.

Designation as a CII obliges an entity to meet a series of standards set by a CII's respective regulator, who in turn defines principles and rules for reporting against steps taken in cybersecurity. The first batch of entities labeled CII at the end of 2021 has until the end of 2024 to meet their basic obligations in cybersecurity. Their compliance level and conformity with legal requirements and international standards are to be checked by supervisory bodies through information requests and security audits. A more detailed list of the responsibilities of CII and their supervisory authorities can be found in Annex IV.

There are presently no state-owned energy companies in the list of Category 1 CII, and there are just ten private energy companies in Category 3, as indicated by the Order of the GoG. These 10 are listed in the table below.

Table I: Energy Sector’s Critical Information Infrastructure of Georgia

#	Energy Sector’s CIIs
1	Telasi, JSC
2	Georgian Water and Power, LTD
3	Energo-Pro Georgia, JSC
4	SOCAR Georgia Gas, LLC
5	Achar Energy-2007, LLC
6	Georgian Pipeline Company, Georgian Branch of Foreign Company
7	Georgia Urban Energy, LLC
8	Eastern Energocorporation, LLC
9	Tbilisi Electricity Supply Company (Telmiko), LTD
10	Tbilisi Energy, LLC

4 RECOMMENDATIONS

This assessment of the country's cybersecurity governance framework reveals a need for further improvement. To address these shortcomings, the Program's key recommendations are for the DGA to coordinate amongst other cybersecurity supervisory authorities to:

- **clarify and operationalize the cybersecurity governance framework.** While the ISL does provide a cybersecurity governance and supervision framework on the strategic and operations level, the architecture is not complete, as the roles of important stakeholders (such as GNERC as a sectoral regulatory authority and NSC's coordination mandate) are missing. Coordination, cooperation and information sharing mechanisms between stakeholders are still not fully defined and regulated. The Program recommends harmonizing the inter- and cross-sectoral framework, including setting unified requirements and regulations whose entry into force can be anticipated.
- **formulate rules and a methodology for identifying CII.** Sector-specific criteria may be necessary, when consultations with sectoral regulatory bodies will be important. The identification process should offer a transparent and rational methodology. In the energy sector GNERC can provide cyber authorities with sector-specific knowledge, help them in the process of identifying CII, as well as act as a mediator and facilitator for enhancement of cooperation between energy CII and national cyber supervisory authorities.
- **avoid and address diverging standards, uneven compliance costs across CII categories within the same sector and confusion over regulatory regimes.** Given CII categorization is based on entity incorporation type, this may lead to a situation in which energy sector entities may be designated to different categories of CII (1st or 3rd) and thus be subject to different supervisory regimes and compliance rules. To avoid these ambiguities (at least among energy sector companies) the Program recommends further assessment of the energy cybersecurity governance framework, an analysis of the existing shortfalls and the establishment of a public-private platform of cooperation, coordination and information sharing between energy CII, GNERC, the DGA, OTA and, when necessary, the NCS.
- **enhance proactive cooperation with CII.** Designation as a CII currently entails increased financial costs, adhesion to additional supervision and bureaucratic burdens. This may result in existing or potential CII attempting to avoid inclusion on the list of CII. Global experience shows that the best solution is to design incentive mechanisms to encourage private sector CII to accept their cybersecurity duties. This should involve proactive communication with CII, including free trainings, workshops, exercises, a clearly defined methodology, supporting materials, cyber and InfoSec services, and a facilitated information sharing platform/forum. Many countries support private sector CII by sharing regular sector-specific threat reports and information on vulnerabilities. This gives companies the benefit of a free, sector-specific customized cybersecurity risk assessment and management tools. This will help CII see direct benefits from increased cyber resilience for their companies.
- **expand the list of CII to include missing energy CII entities.** The current list of energy CII does not reflect the cybersecurity concerns of the energy sector. There are remaining sector participants whose information and operation systems warrant inclusion on the CII list. The annexes in this report contain excerpts of a report titled *Identification of Critical Energy Sector Cybersecurity Infrastructure*, which explains the rationale behind an extension of the current list of CII and lists entities which should be deemed CII. These include:
 - Georgian State Electrosystem JSC
 - Engurhesi LTD
 - Vardnili Hydroplant Cascade LTD
 - Khramhesi I JSC and Khramhesi II JSC
 - Vartsikhe 2005 LTD
 - Adjaristsqali Georgia LLC
 - Gardabani Thermal Power Plant LLC and Gardabani Thermal Power Plant 2 LLC

- Georgian International Energy Corporation LLC
- Mtkvari Energy LLC
- Electricity System Commercial Operator (ESCO) JSC
- Georgian Energy Exchange (GENEX) JSC
- Georgian Oil and Gas Corporation (GOGC) JSC
- Georgian Gas Transportation Company (GGTC) LTD

These entities have been selected following an analysis of the energy sector's subsectors. See Annex II and Annex III for a discussion of the key criteria and methodology used to identify these CIIIs in the energy sector.

5 ANNEXES

ANNEX I: DEFINITION OF CRITICAL INFORMATION INFRASTRUCTURE

Critical Information Infrastructure (CII) is a combination of physical and information technology systems, networks, services, and assets which, if interrupted, damaged or destroyed, could have a destructive impact on the health, safety, national security, or economic well-being of citizens or the active functioning of governmental entities. Therefore, CII security is of the utmost importance in protecting national systems and services.

In the last two decades, energy sector infrastructure has transformed into complex, distributed physical systems. This dramatic transformation of systems and infrastructure is due to the introduction and rapid development of fully or partially automated monitoring and control systems. The current situation demands even more cyber security attention for energy systems due to the prevalent use of centralized Supervisory Control and Data Acquisition (SCADA) systems.

Energy systems with highly spread (decentralized) and evolved SCADA systems are the most prone to cyberattacks. A centralized control strategy makes it possible to shut down the entire system or a large segment of the system through the SCADA distributed infrastructure. Therefore, the protection of energy sector CII entities against cyber threats is crucial.

To defend energy systems from cyber threats and attacks, proactive protection techniques and quick restoration plans are essential tools. There are several security strategies to prevent cyberattacks against critical energy sector cybersecurity infrastructures. Recommendations include:

- proper system and network configuration and patch management
- reduction of the attack surface areas and perimeters
- appropriate management of authentication
- application whitelisting
- development of layered networks
- implementation of secure remote access for users
- active monitoring for attack penetration
- executing a prepared response and others

Such tools, techniques and solutions may vary depending on the company profile, infrastructure, and operations. From the cyber security standpoint, it is important to understand companies' work practices and principles, infrastructure arrangements and types of connections to the outside world.

A cybersecurity governance framework should include not only state-owned infrastructure, but also private CII assets.

ANNEX II: METHODOLOGY FOR CRITICAL INFORMATION INFRASTRUCTURE IDENTIFICATION

Energy and Information Communication Technologies (ICT) rank first and second in the European Commission's list of 11 critical sectors respectively. The energy sector is critical because of the extent to which other sectors and a country's economy as a whole may depend on it. Critical assets of the energy sector interact through ICT, making the energy sector even more vulnerable to malign influences.

The methodology below sets a threshold by which to establish whether an energy sector entity should be considered critical information infrastructure or not using two criteria: 1) the potential impact of direct attacks, malfunctioning on the country, city or region and 2) a measure of the potential negative impact an outage of critical infrastructure could have on an energy system itself.

This approach assumes a scenario in which the Georgian power system is operating in 'island mode', i.e. without interconnection to neighboring power systems. In this configuration, Georgia's power system must ensure security of supply relying exclusively on its own generation sources. This scenario identifies companies and assets, the loss of which would cause serious financial loss to the country or power system collapse.

Key CII identified through this methodology are the electricity transmission system operator, distribution system operator, and generation companies. Energy market platforms are also critical as they are digitally connected to the SCADA, energy management and metering system of critical infrastructure.

The gas sector is examined through the lens of the risk of non-supply of gas to critical infrastructure and facilities, including Thermal Power Plants (TPPs). Gas sector CII include extraction, transmission, distribution systems and storage. For Georgia, only transmission and distribution systems are critical, as the country does not have either gas extraction or storage systems.

ANNEX III: CIIS IN THE GEORGIAN ENERGY SECTOR

POWER SYSTEM CRITICAL INFRASTRUCTURE

A power system is a complex network of generation, distribution and transmission systems, market operations as well as consumption, import and export of electricity. All these subsystems are highly prone to cyber threats due to their structure, functions, and operating philosophy.

The transmission system is the backbone of the power system. Disconnection of the transmission infrastructure element may be caused by a targeted cyberattack. In the isolated island mode, the unplanned outage of any 500 kilovolt (kV) lines or 220 kV lines can cause severe system disturbance and potential system failure. If a cyberattack occurs at several nodes simultaneously, the system will collapse. Under these circumstances, the transmission infrastructure of Georgia (220/330/400/500 kV transmission lines and substations) is critical and should be considered CII.

The distribution system provides town, cities, and regions with power. A targeted cyberattack on the distribution network can lead to the shutdown of a large segment or segments of the electrical power system. These shutdowns can cause unstable transients in power systems, potentially resulting in a system blackout. According to the Ten-Year Network Development Plan (TYNDP) of Georgia, the critical capacity which could stress the system in isolated island mode is 100 megawatts (MW). Therefore, distribution infrastructure should be considered CII.

Generation facilities and power plants should also be considered CII, as they are the main sources of electricity in power systems. The sudden outage of a large generation unit in a small system such as that of Georgia could lead to a rapid decrease in frequency and unstable transient processes with power oscillations. The greater the capacity of the lost generation, the bigger the probability of partial or complete shutdown of the system. It is thus important to identify large power plants as CII. Georgia's TYNDP states that when operating in island mode, the sudden loss of generating units with a capacity greater than or equal to 100 MW can cause severe disturbances to the Georgian power system. Therefore, all power plants and generation units with such capacity should be identified as CII.

Electricity market operators also need to be identified as critical cybersecurity infrastructure as market platforms are accessed online and have digital connections to the SCADA/EMS systems and metering systems of other critical infrastructures in the electricity sector. The shutdown or malfunction of electricity markets can cause serious financial losses associated with inaccuracy or lack of data coming from different market players.

GAS SYSTEM CRITICAL INFRASTRUCTURE

The modern gas industry infrastructure depends heavily on automation for a variety of different operations. This makes them prone to cyber threats. A cyberattack on gas infrastructure can cause serious system malfunctions, faults and leave large cities and regions without gas supply. Georgia does not have its own significant gas resources (less than 0.5% of total annual consumption) and imports gas from neighboring countries. The main supplier is Azerbaijan, which covers about 90% of the country's total gas consumption.

Gas transmission system. Two main gas pipelines are responsible for gas transit in Georgia: the South Caucasus Pipeline (SCP) and the North-South Main Gas Pipeline (NSMP). The SCP transits gas produced from Azerbaijan to Turkey. The NSMP transits Russian gas to Armenia. Gas in Georgia is used for the gas distribution network, thermal power plants, and factories which use gas as an energy input in their operations. The natural gas transportation system in Georgia is owned by the Georgian Oil and Gas Corporation JSC (GOGC) and operated by the Georgian Gas Transportation Company LLC (GGTC) which is a state-owned enterprise and the natural gas transportation licensee. The gas transmission system should be considered a CII from the power system point of view as its malfunction or shutdown would cause TPPs and industrial facilities to go offline.

Gas distribution system. The gas distribution system in Georgia has two major components: one is responsible for supplying the capital of Georgia, Tbilisi, and the other is to supply the rest of the country.

The owner and operator of the largest part of the Tbilisi gas distribution system is Tbilisi Energy. The Tbilisi gas supply has no direct connection with the Georgian power system. The city population primarily uses gas for heating, hence the disruption of the gas distribution system, especially in winter, leaves the city without a major source for heating. This occurrence would normally create a switch to electrical heating. This would in return increase the power system loading peak in winter.

Exactly the same logic can be applied to the regional distribution system where the only supplier is SOCAR.

The gas distribution infrastructure that feeds the capital and regions of Georgia should be deemed CII.

PROPOSED CRITICAL INFORMATION INFRASTRUCTURE ENTITIES OF GEORGIA

Based on the criteria and the logic developed above for each subsector and subsystem, Table 2 is a list of Georgian energy entities which should be considered for inclusion on the list of CIIs.

Table 2: List of Proposed Entities for Addition to CII List

ORGANIZATION	ASSETS	STATUS
Power System		
TRANSMISSION		
Georgian State Electrosystem JSC (GSE)	500, 400, 330, 220 kV lines and substations and Akhaltsikhe HVDC substation	owns and operates
GENERATION		
Engurhesi LTD	Enguri Hydro Power Plant (HPP) – 1300 MW	owns and operates
Vardnili Hydroplant Cascade LTD	Vardnili HPP – 220 MW	owns and operates
Khramhesi I JSC	Khrami HPP 1 – 112.8 MW	owns and operates
Khramhesi II JSC	Khrami HPP 2 – 110 MW	owns and operates
Vartsikhe 2005 LTD	Vartsikhe HPP – 184 MW	owns and operates
Adjaristsqali Georgia LLC	Shuakhevi HPP – 178.72 MW	owns and operates
Gardabani Thermal Power Plant LLC	Gardabani combined cycle power plant (CCGT) – 231.2 MW	owns and operates
Gardabani Thermal Power Plant 2 LLC	Gardabani CCGT 2 – 230 MW	owns and operates
Georgian International Energy Corporation LLC	Tbilsresi – 270 MW	owns and operates
Mtkvari Energy LLC	Gardabani Energy Unit N9 – 300 MW	owns and operates
MARKET OPERATORS		
Electricity System Commercial Operator JSC	Market platform	owns and operates
Georgian Energy Exchange JSC	Day-ahead and Intraday market platform	From 2022
Georgian State Electrosystem JSC	Balancing and Ancillary Services Market platform	From 2022
Gas System		
TRANSMISSION		
Georgian Oil and Gas Corporation JSC	Main gas pipeline system of Georgia	owns
Georgian Gas Transportation Company LTD	Main gas pipeline system of Georgia	operates

ANNEX IV: KEY CII OBLIGATIONS, SUPERVISORY AUTHORITY RESPONSIBILITIES

Additional responsibilities of CII and their supervisory authorities are listed here below:

- Among other mandates, sectoral supervisory authorities set 'Minimum Requirements for Information Security Policies' based on International Organization for Standardization (ISO) or National Institute of Standards and Technology (NIST) standards, with which CII must comply when adopting their internal security regulations, which are determined by a risk assessment-based approach. CII entities have until the end of 2024 to comply with their new obligations. Compliance and conformity with legal requirements and international standards will be checked by supervisory bodies through information requests and security audits.
- Sectoral cybersecurity supervisory authorities issue rules and processes for information asset management based on risk assessment and related security controls. CII use these rules as guidance when taking inventory of their information assets and label them accordingly as confidential, internal use, or public-level assets.
- Rules and frequency of penetration testing of the CII's information systems are also defined by the secondary legislation. CII are required to perform penetration testing and provide detailed reports of identified threats and vulnerabilities to their supervisory authorities.
- Network monitoring sensors are an important tool as a part of the CII's cybersecurity protection measure. Supervisory authorities define the rules for network sensors' configuration, however installation of network sensors is mandatory only for the 1st category of CII. For the other categories of CII, installation of the network sensors is done on a voluntary basis, in conformity with the rules and procedures agreed with supervisory authorities.
- In addition to abovementioned information and cybersecurity rules, category I CII are subject to IT infrastructure inspection.
- A classified information exchange system will be provided as a security measure for voluntary use by non-public entities, while it will be mandatory for public CII.
- Timely notification of cybersecurity incidents to the respective Computer Emergency Response Teams (CERT) of the relevant supervisory authorities is an obligation for all categories of CII.
- Enforcement of the legal obligations based on ISL as well as executing administrative sanctions are carried out either by the supervisory bodies directly or through sector-specific regulatory institutions.
- In accordance with the ISL, each CII entity is obliged to designate two specialists – an Information Security Manager and a Cybersecurity Specialist. These personnel are to be responsible for the day-to-day performance of information and cybersecurity tasks. The roles, responsibilities, qualifications, scope of competences, and certification requirements for an Information Security Manager within CII are defined by the responsible supervisory authorities.
- Supervisory authorities define scope, principles, authorization for conducting an audit, and audit reporting rules for CII to be followed by the Information Security Auditor. They check compliance of CII with the applicable legal requirements and mandatory rules to follow. DGA sets procedures for authorization of persons / organizations entitled to conduct an information security audit and penetration tests within CII. Among other requirements, Information Security Auditors designated to perform a CII's InfoSec audit must be a certified Information Security Auditor (Information Systems Audit and Control Association's [ISACA] CISA Certification).

ANNEX V: REFERENCES

1. The list of 1st, 2nd and 3rd Categories of Critical Information Infrastructures, promulgated by Prime-Minister's Order of 31st December 2021
2. Information Security Law of Georgia
3. On approval of the National Security Council Office's Statute
4. Law of Georgia on Personal Data Protection
5. Law of Georgia on LEPL Operative-Technical Agency of Georgia
6. Law of Georgia on LEPL Digital Governance Agency of Georgia
7. European Union Agency for Cybersecurity

The USAID Securing Georgia's Energy Future Program

Deloitte Consulting Overseas Projects LLP

Address: 80, I. Chavchavadze Avenue, 0162, Tbilisi